
Wie Ihnen Phishing von Zugangsdaten fast egal sein kann.
Tipps und Tools für mehr IT-Sicherheit

AGENDA.

- Motivation
- Kurzvorstellung W&B
- Aufbau des Workshops
- Schutzniveaus – Erläuterungen anhand von 4 Musterunternehmen
- Fazit

Motivation – Warum sind wir hier?

Die Lage der IT-Sicherheit in Deutschland 2024

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland informiert das BSI jährlich über die Bedrohungslage im Cyberraum. Im Bericht für das Jahr 2024 kommt die Cybersicherheitsbehörde des Bundes zur Einschätzung: Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend.

Quelle:
Bundesamt für Sicherheit in der Informationstechnik, 2024

Motivation – Warum sind wir hier?

- Bedrohungslage hoch
  - BSI sieht insbesondere bei KMU dringenden Handlungsbedarf
  - je schlechter Organisationen sich schützen, desto eher werden sie Ziel von Angriffen
  - Cybercrime ist gut organisierte Industrie, die effizient und arbeitsteilig vorgeht

Quelle:
Bundesamt für Sicherheit in der Informationstechnik, 2024

Motivation – Warum sind wir hier?

- Mitarbeiterschulungen reichen nicht aus!
  - CTR von Phishing-Mails bei rund 30 %
  - Effektivität von Training wissenschaftlich umstritten
  - wissenschaftlicher Konsens: Training verhindert keine Angriffe

Quelle: Hillman et al. (2023)

Motivation – Warum sind wir hier?

- Schaden nach einem Cyberangriff bedroht Ihre Existenz!
  - jedes vierte betroffene Unternehmen muss Betriebs-unterbrechungen in Kauf nehmen
  - fast ¾ der Angriffe verursachen erheblichen Schaden
  - jedes fünfte Unternehmen in Zahlungsfähigkeit bedroht

Quelle:
(Hiscox, 2022), (Cyberangriffe KMU: Ergebnisse der HDI Cyber-Studie, 2022)

Vorstellung W&B GmbH

- David Leeuwestein
  - IT-Sicherheitsexperte
- Gründung: 1995
- inhabergeführtes Unternehmen: Frank Winsel, Thomas Blöß, Sönke Wehrend
- Hauptsitz in Lübeck
- Geschäftsbereiche: IT-Systemhaus, Dental Service, Medical Service
- über 70 Mitarbeiter

Hauptsitz Lübeck

Vorstellung W&B GmbH

- IT-Security Konzepte:
  MDR und SOC, EDR, Multi-Faktor-Authentifizierung/Passkeys, Backup, Firewall, Monitoring, Patch-Management, etc.
- IT-Infrastrukturkonzepte:
  Projektplanung/Konfiguration, Produkte, Betreuung
- Managed-IT-Service:
  Helpdesk, Monitoring, Dokumentation, etc.
- Kommunikationskonzepte

Aufbau des Workshops – was erwartet Sie?

- Vorstellung verschiedener Schutzniveaus anhand von 4 fiktiven Muster-Unternehmen
- vor jedem Muster-Unternehmen anonyme Umfrage
  - ehrlich antworten ☺
- Erläuterung der Schutzniveaus
  - Was ist gut?
  - Was ist verbesserungswürdig?

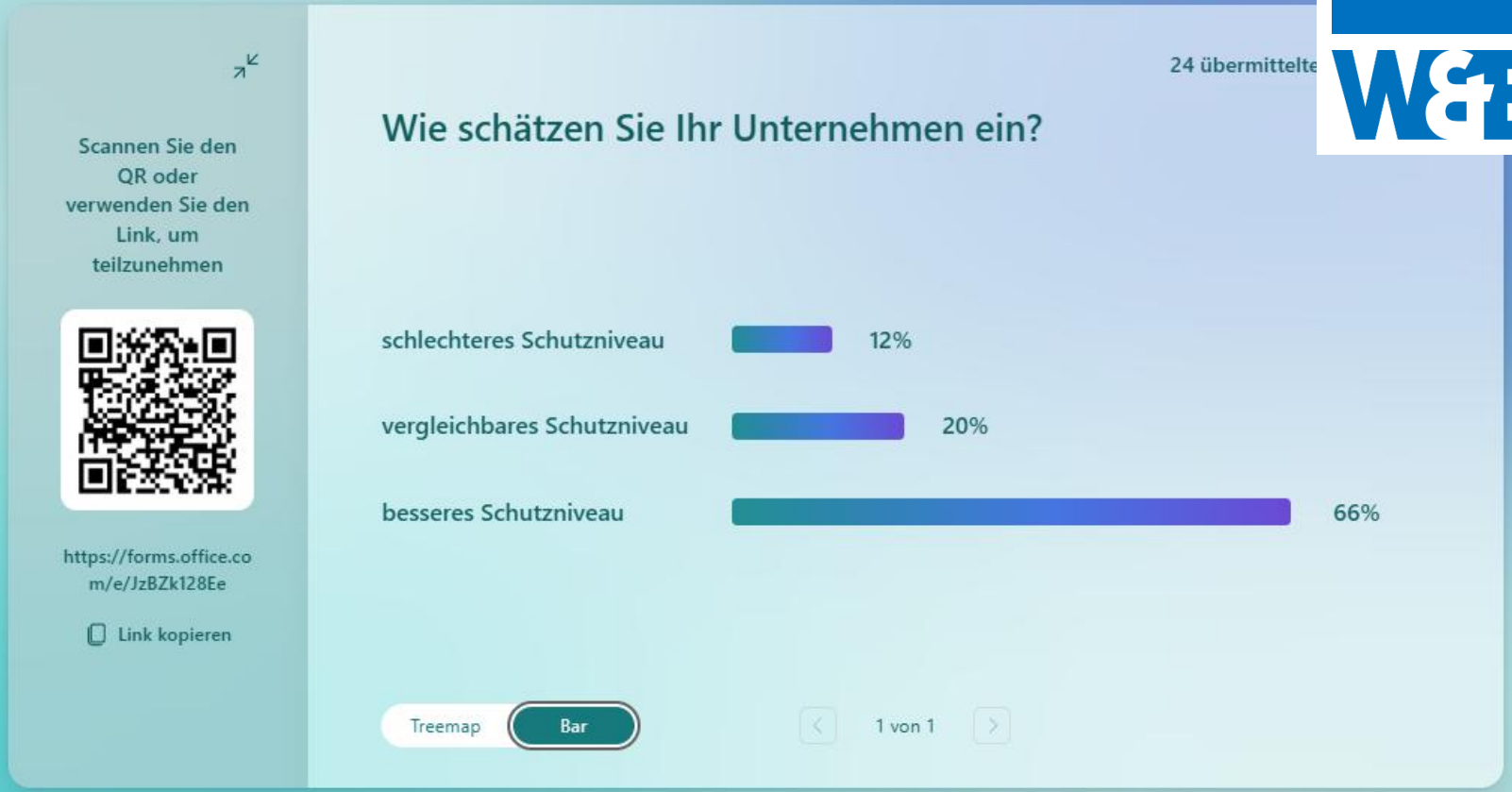
Schutzniveau 0: Müller Maschinenbau GmbH „Alle dürfen alles“

- ein Postfach/ein Passwort für alle
- Anmeldung an den lokalen Arbeits-geräten mit lokalen Benutzern
- ggf. werden auch private Geräte für die Arbeit verwendet

Dieses Schutzniveau hat hoffentlich niemand mehr!

Schutzniveau 1: Schneider Textilwerke AG „Mit IT-Sicherheit haben wir uns doch schon vor 20 Jahren beschäftigt.“

- zentrale Account-Verwaltung
- persönliche Accounts für Mitarbeitende
- delegierte Postfächer
- aber keine Multifaktor-Authentifizierung, keine Passkeys



Umfrage

Schutzniveau 1: Schneider Textilwerke AG

„Mit IT-Sicherheit haben wir uns doch schon vor 20 Jahren beschäftigt.“

Schutzniveau 1: Schneider Textilwerke AG „Mit IT-Sicherheit haben wir uns doch schon vor 20 Jahren beschäftigt.“

Warum ist das gut?

- ☺ geht ein Mitarbeitender, kann sein Konto einfach gesperrt werden
- ☺ wird bspw. eine Phishing-Mail zugestellt, ist klar, an wen sie gegangen ist -> Auditierbarkeit

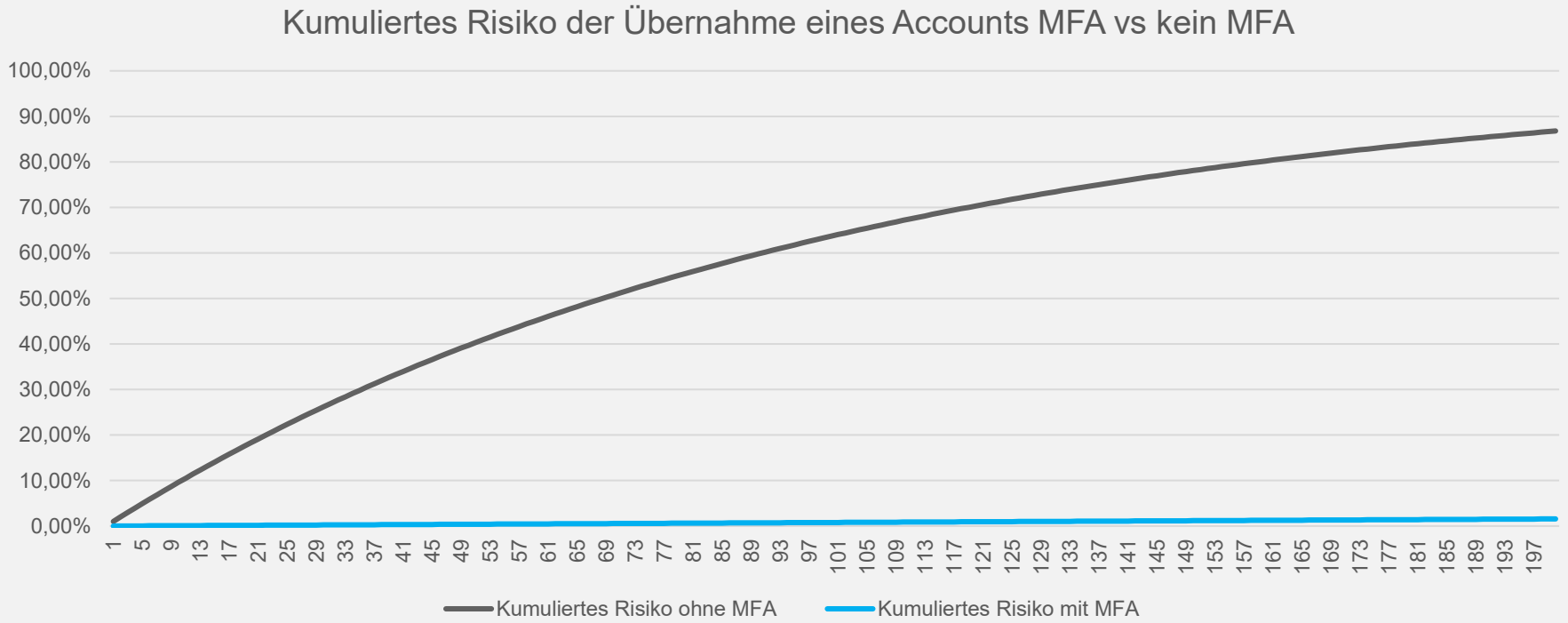
Schutzniveau 1: Schneider Textilwerke AG „Mit IT-Sicherheit haben wir uns doch schon vor 20 Jahren beschäftigt.“

Warum ist das schlecht?

☹ kein Schutz gegen Phishing

Schutzniveau 1: Schneider Textilwerke AG

Warum ist das schlecht? ☹ Studie von Microsoft zeigt:



Prozentuale Wahrscheinlichkeit, dass in einem Zeitraum von 6 Monaten mindestens ein Account einer Organisation kompromittiert wird, abhängig von der Anzahl der Firmen-Accounts (ausgehend von stoch. unabh. Zufallsereign.).

Quelle: Meyer et al. (2023)

Scannen Sie den QR oder verwenden Sie den Link, um teilzunehmen

https://forms.office.com/e/nFvwJGA0Rf

Link kopieren

23 übermittelte

Nutzen Sie für jeden Dienst ein anderes Passwort?

Treemap | Bar

1 von 1

Umfrage

Schutzniveau 1: Schneider Textilwerke AG

„Mit IT-Sicherheit haben wir uns doch schon vor 20 Jahren beschäftigt.“

Schutzniveau 1: Schneider Textilwerke AG „Mit IT-Sicherheit haben wir uns doch schon vor 20 Jahren beschäftigt.“

Warum ist das schlecht?

- ☹ kein Schutz gegen Phishing
- ☹ geklaute Zugangsdaten können missbraucht werden

Test:
haveibeenpwned.com

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

Lead Hunter: In March 2020, a massive trove of personal information referred to as "Lead Hunter" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The data contained 69 million unique email addresses across 110 million rows of data accompanied by additional personal information including names, phone numbers, genders and physical addresses. At the time of publishing, the breach could not be attributed to those responsible for obtaining and exposing it. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Genders, IP addresses, Names, Phone numbers, Physical addresses

Epik: In September 2021, the domain registrar and web host Epik suffered a significant data breach, allegedly in retaliation for hosting alt-right websites. The breach exposed a huge volume of data not just of Epik customers, but also scraped WHOIS records belonging to individuals and organisations who were not Epik customers. The data included over 15 million unique email addresses (including anonymised versions for domain privacy), names, phone numbers, physical addresses, purchases and passwords stored in various formats.

Compromised data: Email addresses, Names, Phone numbers, Physical addresses, Purchases

Schutzniveau 2: Schmidt & Söhne Bau KG „Wir glauben, IT-Sicherheit gut umzusetzen, haben das aber nie von Experten prüfen lassen.“

- nutzt alles, was in Schutzniveau 1 auch genutzt wird, plus
  - zentrale Accountverwaltung, zum Beispiel über Microsoft 365 (Entra)
  - einfache Multifaktor-Authentifizierung (MFA), z. B. durch SMS, App, TOTP

Scannen Sie den QR oder verwenden Sie den Link, um teilzunehmen

https://forms.office.com/e/mTFxEyL8DS

Link kopieren

21 übermittelte

Wie schätzen Sie Ihr Unternehmen ein?

Treemap | Bar

1 von 1

Umfrage

Schutzniveau 2: Schmidt & Söhne Bau KG / „Wir glauben, IT-Sicherheit gut umzusetzen, haben das aber nie von Experten prüfen lassen.“

Schutzniveau 2: Schmidt & Söhne Bau KG „Wir glauben, IT-Sicherheit gut umzusetzen, haben das aber nie von Experten prüfen lassen.“

Warum ist das gut?

- ☺ wie in der Grafik zuvor gesehen: MFA reduziert das Phishing-Risiko um bis zu 99,22 %
- ☺ sehr viel besser -> die meisten Firmen schaffen dieses Niveau nicht

Schutzniveau 2: Schmidt & Söhne Bau KG „Wir glauben, IT-Sicherheit gut umzusetzen, haben das aber nie von Experten prüfen lassen.“

Warum ist das schlecht?

- ☹ kein perfekter Schutz gegen Phishing
- ☹ leicht zu hacken, wie dieses Video beweist…

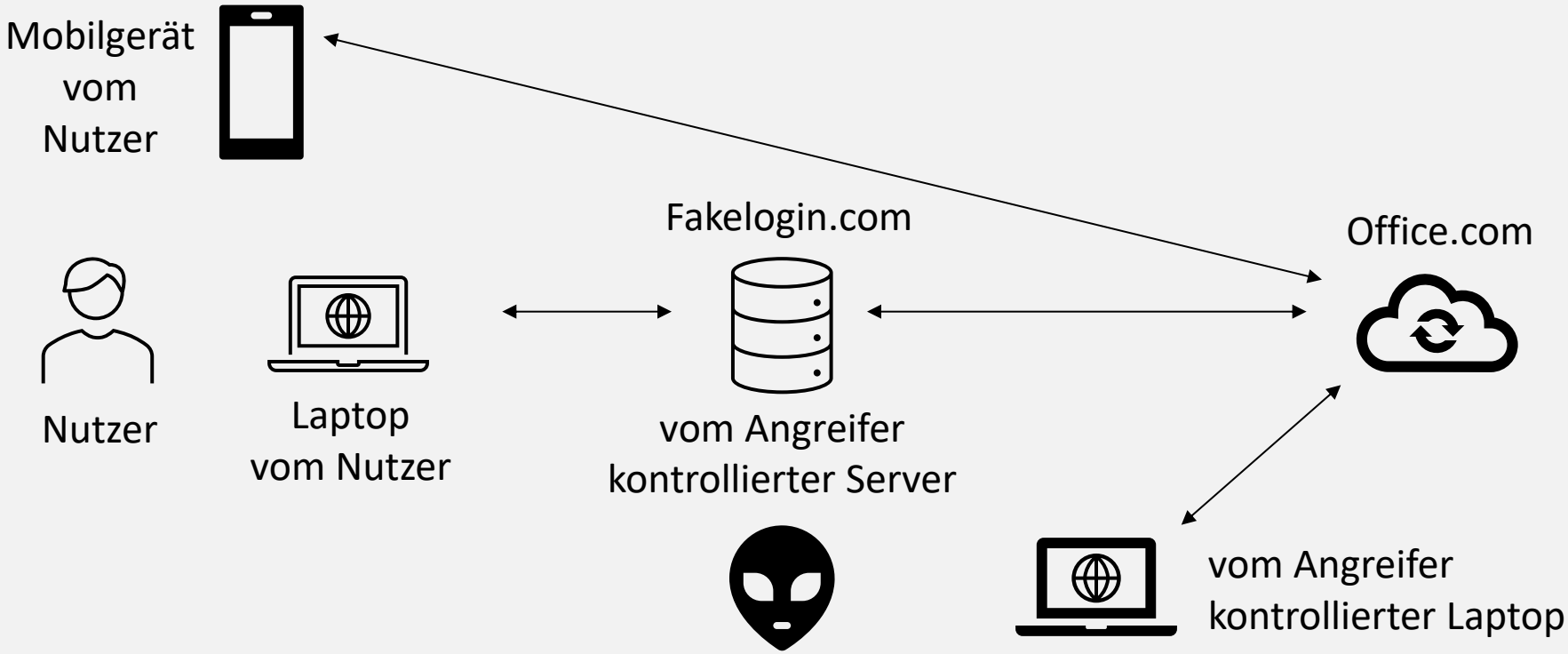
Adversary in the Middle (AiTM)

Evilginx vs. Microsoft Authenticator

Quelle: YouTube Video „AiTM Demo Evilginx vs Microsoft Authenticator“
Klicken Sie hier, um direkt zu YouTube zu gelangen:
https://www.youtube.com/watch?v=5rUbRJqUCpE&t=177s

getidee.com

Schutzniveau 2: Schmidt & Söhne Bau KG



Schutzniveau 3: Krause Elektronik GmbH „Wir wurden schon gehackt, jetzt tun wir alles, damit das nicht wieder passiert!“

- … hätten wir mal früher reagiert!
- nutzt alles, was in Schutzniveau 1 und 2 auch genutzt wird, plus
  - Verwendung von Passkeys

Scannen Sie den QR oder verwenden Sie den Link, um teilzunehmen

https://forms.office.com/e/Hk0mnGb2fX

Link kopieren

19 übermittelte

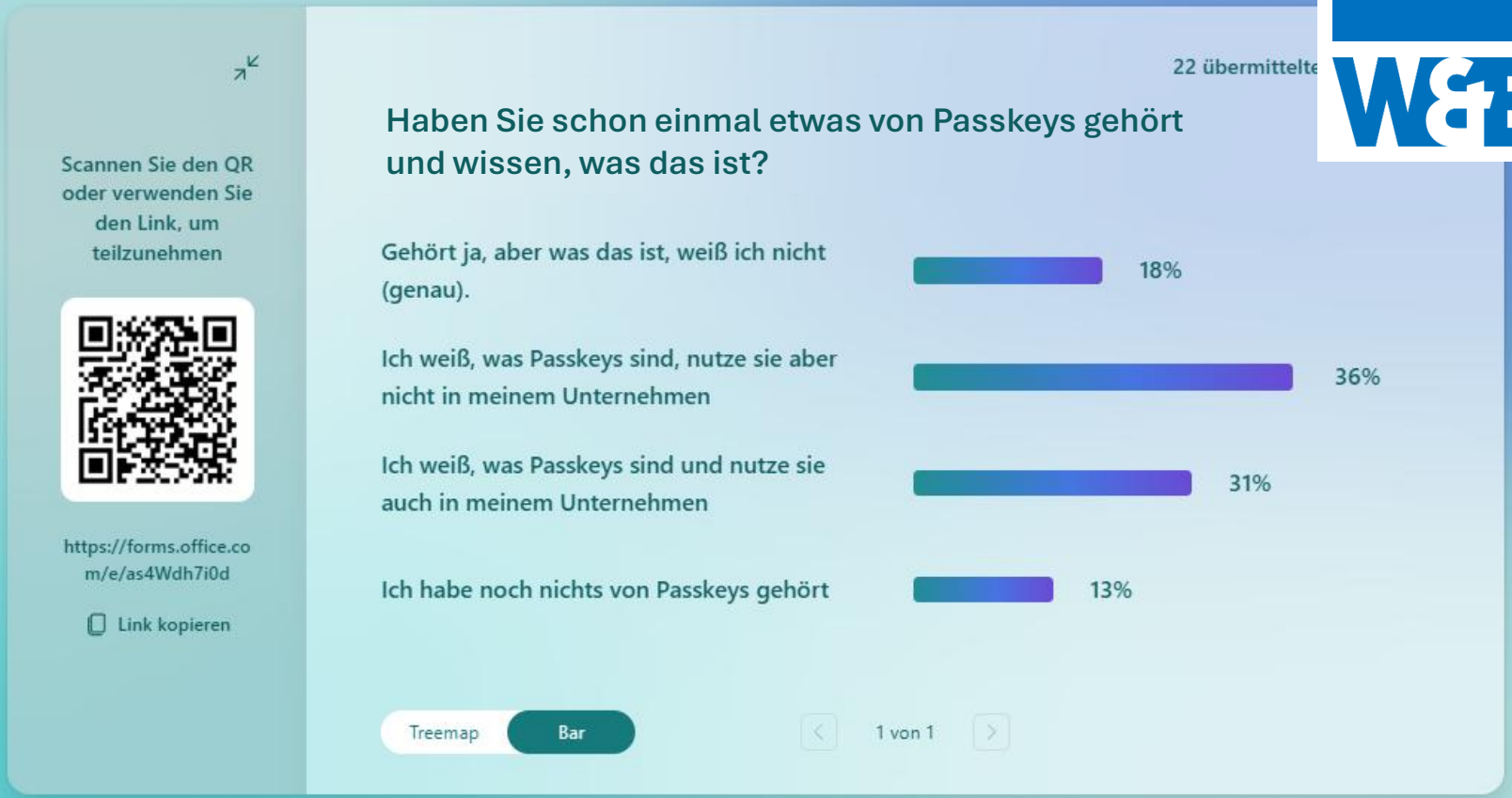
Wie schätzen Sie Ihr Unternehmen ein?

Treemap | Bar

1 von 1

Umfrage

Schutzniveau 3: Krause Elektronik GmbH / „Wir wurden schon gehackt, jetzt tun wir alles, damit das nicht wieder passiert!“

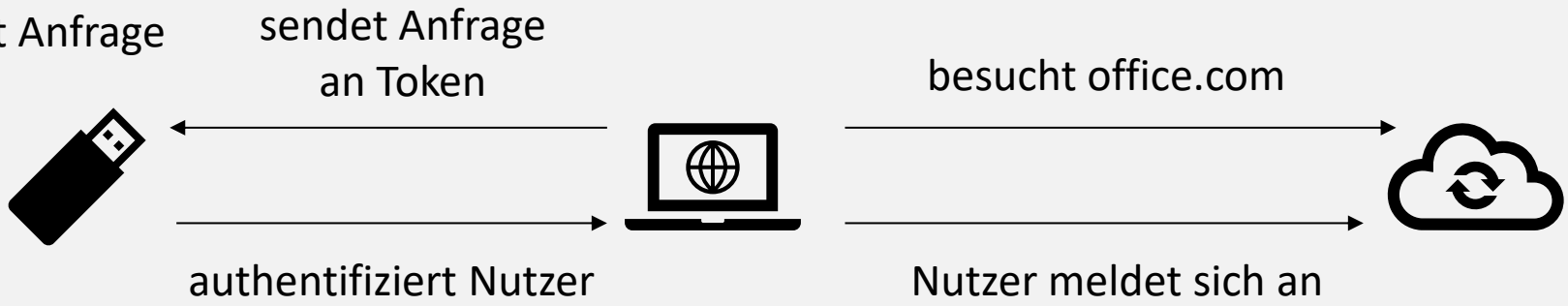


Umfrage

Schutzniveau 3: Krause Elektronik GmbH / „Wir wurden schon gehackt, jetzt tun wir alles, damit das nicht wieder passiert!“

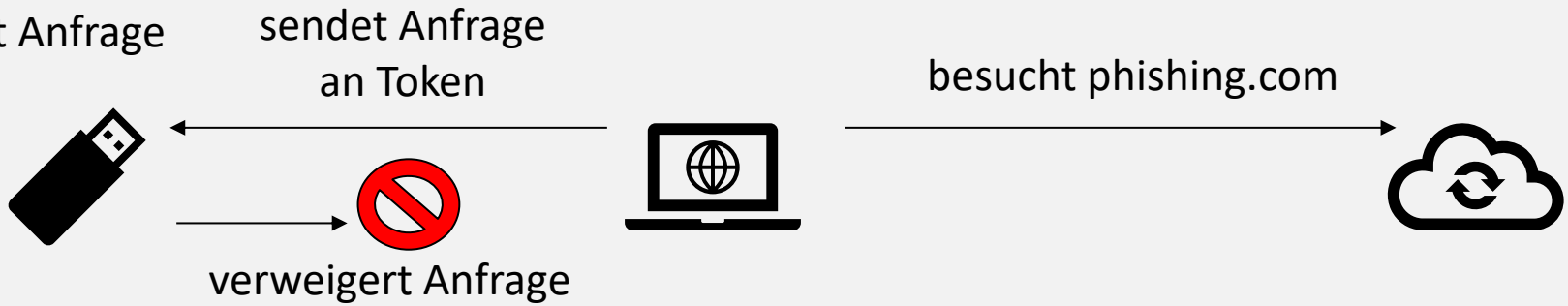
Schutzniveau 3: Krause Elektronik GmbH

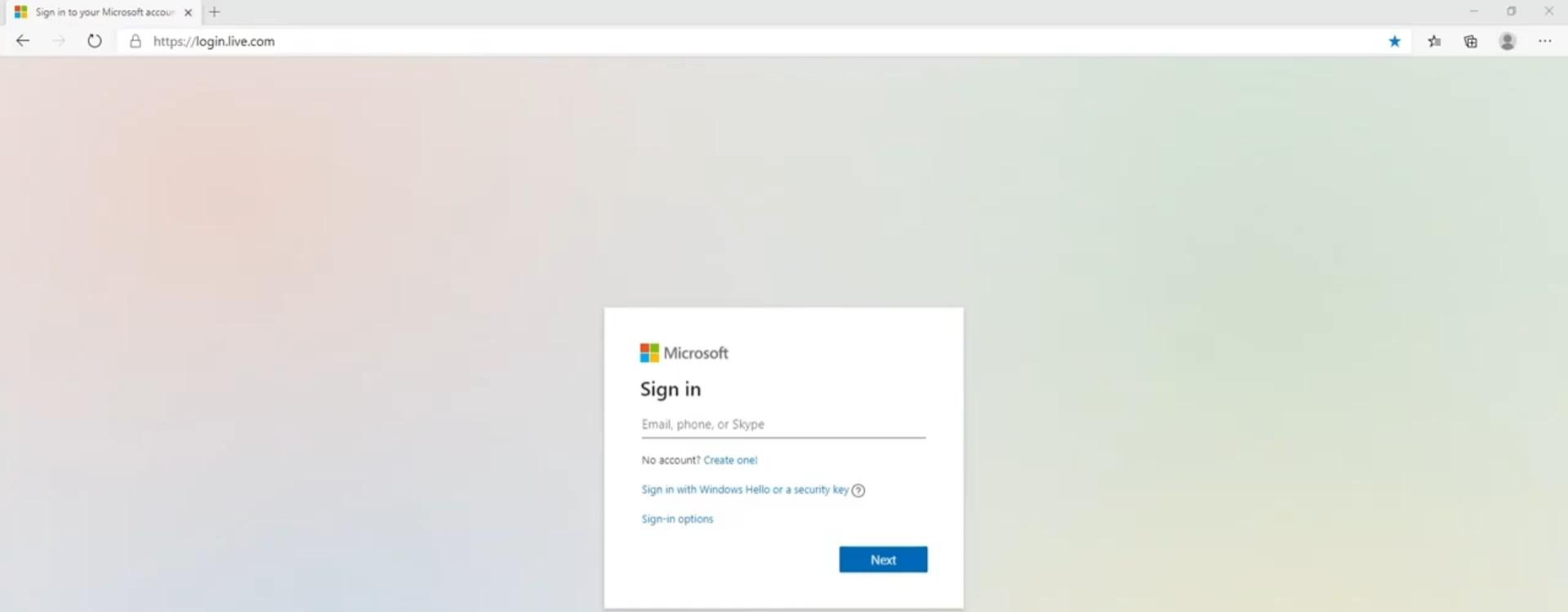
Passkeys 101



Schutzniveau 3: Krause Elektronik GmbH

Passkeys 101





*Quelle: YouTube Video „*How-to_ Go Passwordless with Microsoft Accounts & YubiKey*“*
Klicken Sie hier, um das Video direkt bei YouTube abzuspielen: https://www.youtube.com/watch?v=sI7yWHim-2Y&t=32s

Schutzniveau 3: Krause Elektronik GmbH „Wir wurden schon gehackt, jetzt tun wir alles, damit das nicht wieder passiert!“

Warum ist das gut?

- ☺ Phishing von Zugangsdaten unmöglich
- ☺ einzige hier vorgestellte Anmelde-methode, die vom Bundesamt für Sicherheit in der Informations-technik (BSI) empfohlen wird
- ☺ sehr hohes Schutzniveau

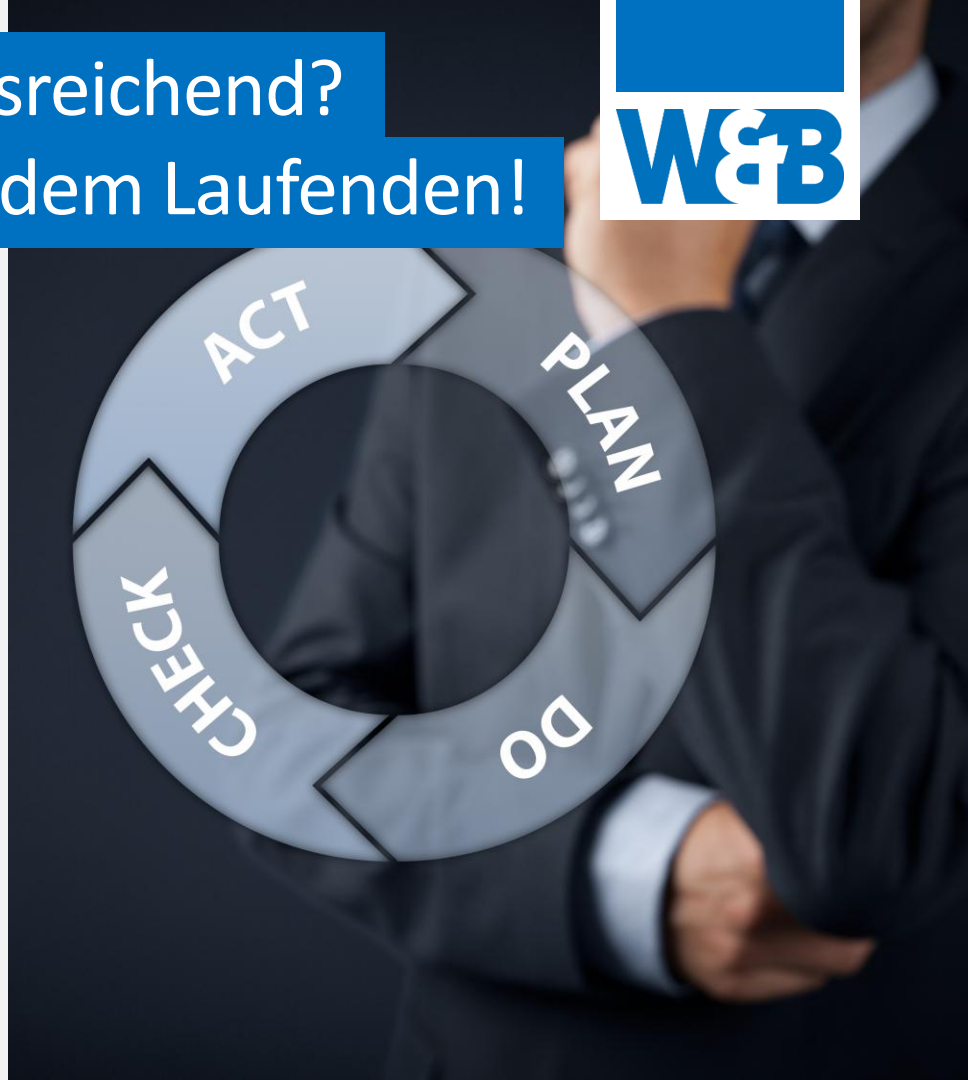
Schutzniveau 3: Krause Elektronik GmbH „Wir wurden schon gehackt, jetzt tun wir alles, damit das nicht wieder passiert!“

Warum ist das schlecht?

- ☹ weitere Angriffsvektoren bleiben möglich
- ☹ Hardwaretoken kann verloren gehen
- ☹ Gerät kann gehackt werden

Fazit: Ist Schutzniveau 3 ausreichend? NEIN! Bleiben Sie stets auf dem Laufenden!

- Man sollte immer auf dem Laufenden bleiben und sich informieren, denn Cyberangriffe und die Schutzmaßnahmen entwickeln sich stetig weiter!
- Haben Sie zum Beispiel schon von EDR und MDR gehört?
- **Es gibt einfache und verlässliche Möglichkeiten, sich zu schützen. Werden Sie aktiv!**

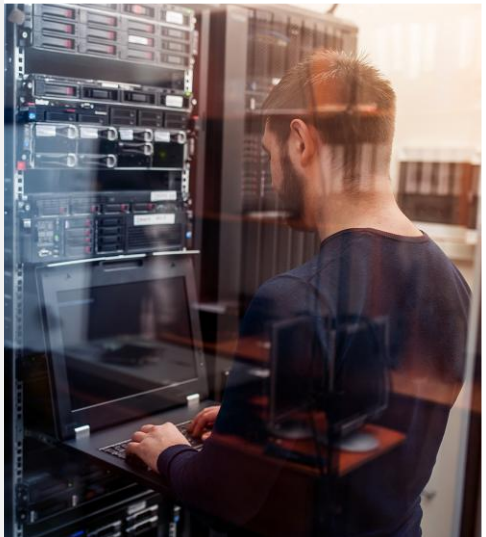


Sie möchten mehr wissen?

Wir freuen uns auf Ihren Kontakt und beraten Sie gerne unverbindlich!

W&B GmbH - IT-Systemhaus
Steinmetzstraße 7 | 23556 Lübeck
www.wb-systemhaus.de

David Leeuwestein
IT-Sicherheitsexperte
(0451) 39988-300
beratung@wb-net.de



Quellen

- Bitkom. (2024, 27. September). Angriffe auf die deutsche Wirtschaft nehmen zu. Bitkom. https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024
- Bundesamt für Sicherheit in der Informationstechnik. (2024). Die Lage der IT-Sicherheit in Deutschland. Abgerufen am 12. Dezember 2024, von https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
- Cyberangriffe KMU: Ergebnisse der HDI Cyber-Studie. (2022, 12. April). hdi.de. Abgerufen am 12. Dezember 2024, von https://www.hdi.de/konzern/presse/cyberangriffe-und-schaeden-bei-kmu/
- Hillman, D., Harel, Y. & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. Computers & Security, 132, 103364. https://doi.org/10.1016/j.cose.2023.103364
- Hiscox. (2022). Cyber Readiness Report 2022. Abgerufen am 12. Dezember 2024, von https://www.hiscox.co.uk/sites/default/files/documents/2022-08/Hiscox-UK-Cyber-Readiness-Report-2022.pdf
- Meyer, L. A., Romero, S., Bertoli, G., Burt, T., Weinert, A. & Ferres, J. L. (2023). How effective is multifactor authentication at deterring cyberattacks? arXiv (Cornell University). https://doi.org/10.48550/arxiv.2305.00945

YouTube Videos

AiTM Demo Evilginx vs Microsoft Authenticator: https://www.youtube.com/watch?v=5rUbRJqUCpE&t=177s

Anmeldung via Passkey (How-to_ Go Passwordless with Microsoft Accounts & YubiKey): https://www.youtube.com/watch?v=sI7yWHim-2Y&t=32s